REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-9, 12-15, 17, 21-25, 28, and 31 are currently pending in this application. Claims 1 and 21 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 21.

Claim Objections

Claims 14 and 15 are objected to for incorrect dependencies. Claims 14 and 15 have been amended to depend from independent claim 1 according to the Examiner's suggestions. Thus, withdrawal of this objection is respectfully requested.

Rejections under 35 U.S.C. § 102

Claims 1-5, 21, and 22 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,870,474 ("Wasilewski"). Although the rejection on page 3 of the Office Action mailed December 6, 2005, lists only claims 1-5, 21, and 22 as being rejected under 35 U.S.C. § 102(b), Applicant believes the Examiner meant to include claims 6, 7, 12-15, and 17 in the rejection. Thus, Applicant has written this response under the assumption that claims 6, 7, 12-15, and 17 are also rejected under 35 U.S.C. § 102(b) as being anticipated by Wasilewski. With respect to these claims, this rejection is respectfully traversed.

In the claimed invention, as recited in independent claims 1 and 21, one or more precalculated key pairs are stored in the memory of the decoder, where each key pair comprises

a session key and an encrypted version of the same session key. The encrypted version of the session key is obtained using a transport key. The encrypted value of the session key is communicated to the portable security module, which decrypts the value using the transport key *stored in the memory of the portable security module.* That is, the portable security module *stores a copy of the transport key* and uses the transport key it has to decrypt the encrypted session key. Further, all subsequent data that is communicated between the decoder and the portable security module is encrypted and decrypted using the session key that both the decoder and the portable security module now can access.

Turning to the rejection of the claims, for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. The Application respectfully asserts that Wasilewski fails to disclose or suggest all of the limitations of the claimed invention.

In contrast to the invention recited in claims 1 and 21, Wasilewski discloses three levels of encryption used to transmit a program from a service provider (SP) to a customer's set top box (STU). First, the program (containing MPEG-2 transport packets) is encrypted using control words (*i.e.,* randomly generated keys). Second, the control words are encrypted using a second randomly generated key, called a multi-session key (MSK) in Wasilewski. The MSK is then encrypted using public cryptography methods (*see* Wasilewski, col. 8, ll. 1-7). In Wasilewski, the MPEG-2 transport stream is sent from a service provider to a customer's set top box (STU). The STU undoes the three levels of encryption as follows. First, the STU decrypts the MSK using its own private key corresponding to its public key used to encrypt the MSK (*see* Wasilewski, col. 8, ll. 45-47). Second, the STU decrypts the control words using the now

decrypted MSK. Finally, the STU decrypts the MPEG-2 transport packets using the control words that are sent with the MPEG-2 transport stream.

Wasilewski fails to disclose or suggest the limitations of the invention recited in claims 1 and 21 for at least the following reasons:

(i) Wasilewski is not concerned with encryption of data between a decoder and a portable security module. Rather, Wasilewski discloses encrypting data between a service provider and an STU. In fact, Wasilewski does not even mention any type of security module. The portable security module of the claimed invention is a detachable device that can be inserted into the decoder (e.g., a smart card), as clearly described in the Specification on page 6, ll. 15-17 and page 10, ll. 29-31. Even assuming arguendo that the STU disclosed in Wasilewski is equivalent to the decoder of the claimed invention, it is not possible to equate the SP of Wasilewski with a portable security module, as recited in the claimed invention. A SP is an entity responsible for providing broadband service to the STU, not a detachable device that is used in conjunction with a decoder to provided added security.

(ii) Wasilewski fails to disclose or suggest at least a precalculated key pair that is stored in a decoder. In fact, the only key pair disclosed by Wasilewski is the public/private key pair associated with the STU (see Wasilewski, col. 10, ll. 13-15). However, the public/private key pair is associated with a public cryptography algorithm used to encrypt the MSK (see Wasilewski, col. 8, ll. 37-40). In the claimed invention, the precalculated key pair comprises the session key and an encrypted version of the session key. The keys in the public/private key pair of Wasilewski are not associated with each other like

the precalculated key pair of the claimed invention. That is, in the public/private key pair disclosed in Wasilewski, one key is not the encrypted version of the other key.

Further, assuming *arguendo* that the public/private key pair is equivalent to the precalculated key pair of the claimed invention, the public/private key pair of Wasilewski still does not contain the encrypted version of the session key that is communicated to the portable security module, as required by claims 1 and 21. This is because 1) Wasilewski fails to disclose a portable security module; and 2) neither key in the public/private key pair is communicated to another device. Rather, the whole point of a public/private key pair is that the data is encrypted with the public key (which is *publicly known*) and decrypted with the private key (which no one knows except the entity that decrypts the data). Thus, there is no need to communicate either of the keys in the key pair of Wasilewski to a portable security module (*see* Wasilewski, col. 23, ll. 15-18).

(iii) Wasilewski also fails to disclose or suggest at least a transport key stored in a portable security module that is used to decrypt the encrypted session key. The Examiner cites col. 7, ll. 64 – col. 8, ll. 7 of Wasilewski in asserting that Wasilewski does disclose the aforementioned limitation, however, this is incorrect. Wasilewski discloses that the MSK is encrypted using public cryptography methods, in which case a corresponding *private key* is used to decrypt the MSK. Using a private key corresponding to a public key to decrypt the MSK is distinct from decrypting the session key using a *copy of the same key* that was used to encrypt the session key.

(iv) From the above, it follows that Wasilewski also cannot possibly disclose or suggest at least that a portable security module *stores* a copy of the same key that was used to

encrypt the session key (*i.e.,* the transport key), as recited in independent claims 1 and 21.

(v) Further, Wasilewski fails to disclose or suggest at least that once the session key is decrypted by the portable security module, all subsequent communication between the portable security module and the decoder is performed using the session key that both devices now have in common. In fact, Wasilewski is completely silent with respect to any subsequent communication between the SP and the STU and how that communication is performed.

In view of the above, it is clear that Wasilewski fails to disclose or suggest each and every limitation recited in independent claims 1 and 21. Thus, independent claims 1 and 21 are patentable over Wasilewski. Dependent claims 2-7, 12-15, 17, and 22 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 8 and 24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of the book "Applied Cryptography" by Schneier ("Schneier"). This rejection is respectfully traversed.

As described above, Wasilewski fails to disclose the limitations of independent claims 1 and 21. Further, Schneier fails to supply that which Wasilewski lacks, as evidenced by the fact that the Examiner relies on Schneier solely for the purpose of disclosing a symmetric cryptographic algorithm and an associated symmetric key (*see* Office Action mailed December 6, 2005, page 6). Thus, it is clear that independent claims 1 and 21 are patentable over Wasilewski and Schneier, whether considered separately or in combination. Dependent claims 8

and 24 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 9 and 25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of the book "Applied Cryptography" by Schneier ("Schneier"). This rejection is respectfully traversed.

As described above, Wasilewski fails to disclose the limitations of independent claims 1 and 21. Further, Schneier fails to supply that which Wasilewski lacks, as evidenced by the fact that the Examiner relies on Schneier solely for the purpose of disclosing an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the portable security module corresponds to a symmetric algorithm (*see* Office Action mailed December 6, 2005, page 7). Thus, it is clear that independent claims 1 and 21 are patentable over Wasilewski and Schneier, whether considered separately or in combination. Dependent claims 9 and 25 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 23 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of U.S. Patent No. 5,835,726 ("Shwed"). This rejection is respectfully traversed.

As described above, Wasilewski fails to disclose the limitations of independent claim 21. Further, Shwed fails to supply that which Wasilewski lacks, as evidenced by the fact that the Examiner relies on Shwed solely for the purpose of disclosing that the encrypted version of the session key includes a signature value readable by the portable security module to verify the authenticity of the encrypted session key (*see* Office Action mailed December 6, 2005, page 7). Thus, it is clear that independent claim 21 is patentable over Wasilewski and Shwed, whether

considered separately or in combination. Dependent claim 23 is patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 28 and 31

Applicant notes that the Examiner has not addressed claims 28 and 31 in any way in the Office Action mailed December 6, 2005. However, because these claims depend from independent claim 21, addressed above as being patentable over all prior at of record, Applicant respectfully requests the Examiner to indicate that claims 28 and 31 contain allowable subject matter for at least the same reasons as presented above.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 11345/034001).

Dated: February 6, 2006   Respectfully submitted,
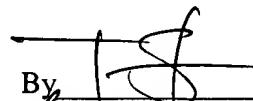
By _____ #45,079
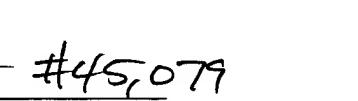
Jonathan P. Osha   THOMAS SCHERER
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

134760_3

13